Nguyen An Khuong



## Contents

Core Programming Language

Hoare Triples: Partial and Total Correctness

Proof Calculus for Partial Correctness

Practical Aspects of Correctness Proofs

Correctness of the Factorial Function

Proof Calculus for Total Correctness

Homeworks

Chapter 2f Program Verification

Mathematical Modeling (CO2011)

(Materials drawn from:

"Michael Huth and Mark Ryan. Logic in Computer Science: Modelling and Reasoning about Systems, 2nd Ed., Cambridge University Press, 2006.")

BỞI HCMUT-CNCP

Nguyen An Khuong

Faculty of Computer Science and Engineering University of Technology, VNU-HCM

# Contents

**Program Verification** 

Nguyen An Khuong



Core Programming Language

Hoare Triples: Partial and Total Correctness

Proof Calculus for Partial Correctness

Practical Aspects of Correctness Proofs

Correctness of the Factorial Function

Proof Calculus for **Total Correctness** 

Homeworks

1 Core Programming Language

2 Hoare Triples; Partial and Total Correctness

3 Proof Calculus for Partial Correctness

4 Practical Aspects of Correctness Proofs

**6** Correctness of the Factorial Function

6 Proof Calculus for Total Correctness

BÓI HCMUT-CNCP

Nguyen An Khuong



# Contents

Core Programming Language

Hoare Triples; Partial and Total Correctness

Proof Calculus for Partial Correctness

Practical Aspects of Correctness Proofs

Correctness of the

Proof Calculus for

Homeworks

KHOACNCD

- One way of checking the correctness of programs is to explore the possible states that a computation system can reach during the execution of the program.
- Problems with this model checking approach:
  - Models become infinite
  - Satisfaction/validity becomes undecidable.
- In this lecture, we cover a proof-based framework for program verification.

BỞI HCMUT-CNCP

# Characteristics of the Approach

Program Verification

Nguyen An Khuong



Contents

Core Programming Language

Hoare Triples; Partial and Total Correctness

Proof Calculus for Partial Correctness

Practical Aspects of Correctness Proofs

Correctness of the

Proof Calculus for

Homeworks

CHK

Proof-based instead of model checking Semi-automatic instead of automatic

Property-oriented not using full specification

Application domain fixed to sequential programs using integers Interleaved with development rather than a-posteriori verification



# **Reasons for Program Verification**

**Program Verification** Nguyen An Khuong



Documentation. Program properties formulated as theorems can

Time-to-market. Verification prevents/catches bugs and can reduce development time

serve as concise documentation

Reuse. Clear specification provides basis for reuse

Certification. Verification is required in safety-critical domains such as nuclear power stations and aircraft cockpits

BỞI HCMUT-CNCP

Core Programming Language

Hoare Triples: Partial and Total Correctness

Proof Calculus for Partial Correctness

Practical Aspects of Correctness Proofs

Correctness of the Factorial Function

Proof Calculus for Total Correctness

# Framework for Software Verification

**Program Verification** 

Nguyen An Khuong



## Contents

Core Programming Language

Hoare Triples; Partial and Total Correctness

Proof Calculus for Partial Correctness

Practical Aspects of Correctness Proofs

Correctness of the Factorial Function

Proof Calculus for

Homeworks

Convert informal description R of requirements for an application domain into formula  $\phi_R$ .

Write program P that meets  $\phi_R$ .

Prove that P satisfies  $\phi_R$ .

Each step provides risks and opportunities.

# TÀI LIỆU SƯU TẬP BỞI HCMUT-CNCP

Nguven An Khuong



Contents

Core Programming

Hoare Triples: Partial and Total Correctness

Proof Calculus for Partial Correctness

Practical Aspects of Correctness Proofs

Correctness of the

Factorial Function Proof Calculus for

**Total Correctness** 

Homeworks

1 Core Programming Language

Hoare Triples; Partial and

Proof Calculus for Partial Correctness

Practical Aspects of Correctness Proofs

Correctness of the Factorial Function

Proof Calculus for Total Coffectness U'U TÂP

# **Motivation of Core Language**

MHOACNCD

- Real-world languages are quite large; many features and constructs
- Theoretical constructions such as Turing machines or lambda calculus are too far from actual applications; too low-level
- Idea: use subset of Pascal/C/C++/Java
- Benefit: we can study useful "realistic" examples

TÀI LIỆU SƯU TẬP

BACHKHOACNCP.COM

**Program Verification** 

Nguyen An Khuong



Contents

Core Programming

Hoare Triples; Partial and Total Correctness

Proof Calculus for Partial Correctness

Practical Aspects of Correctness Proofs

Correctness of the

Proof Calculus for

# **Expressions in Core Language**

**Program Verification** 

Nguyen An Khuong



Contents

Core Programming

Hoare Triples; Partial and Total Correctness

Proof Calculus for Partial Correctness

Practical Aspects of Correctness Proofs

Correctness of the Factorial Function

Proof Calculus for Total Correctness

Homeworks

MAHOACNC

Expressions come as arithmetic expressions E:

$$E ::= n \mid x \mid (-E) \mid (E + E) \mid (E - E) \mid (E * E)$$

and boolean expressions B:

$$B ::= \mathtt{true} \mid \mathtt{false} \mid (!B) \mid (B \& B) \mid (B \| B) \mid (E < E)$$

Where are the other comparisons, for example ==?

**B**ổI HCMUT-CNCP

# **Commands in Core Language**

CHKHOACNCX

Commands cover some common programming idioms. Expressions are components of commands.

$$C ::= x = E \mid C; C \mid \texttt{if} \ B \ \{C\} \ \texttt{else} \ \{C\} \mid \texttt{while} \ B \ \{C\}$$

# TÀI LIỆU SƯU TẬP

BACHKHOACNCP.COM

**Program Verification** 

Nguyen An Khuong



Contents

Core Programming

Hoare Triples; Partial and Total Correctness

Proof Calculus for Partial Correctness

Practical Aspects of Correctness Proofs

Correctness of the Factorial Function

Proof Calculus for Total Correctness

# Nguyen An Khuong



# Contents

# Core Programming

Hoare Triples; Partial and Total Correctness

Proof Calculus for Partial Correctness

Practical Aspects of Correctness Proofs

Correctness of the

Factorial Function

Proof Calculus for Total Correctness

Homeworks

KHOACNCX

Consider the factorial function:

$$\begin{array}{ccc}
0! & \stackrel{\text{def}}{=} & 1 \\
(n+1)! & \stackrel{\text{def}}{=} & (n+1) \cdot n!
\end{array}$$

We shall show that after the execution of the following Core program, we have y=x!.

```
y = 1;
z = 0;
while (z != x) { z = z + 1; y = y * z; } U TÂP
```



# Contents

Core Programming Language

Proof Calculus for Partial Correctness

Practical Aspects of Correctness Proofs

Correctness of the

Factorial Function

Proof Calculus for **Total Correctness** 

Homeworks

Nguven An Khuong

**1** Core Programming Language

2 Hoare Triples; Partial and Total Correctness

Proof Calculus for Partial Correctness

Practical Aspects of Correctness Proofs

Correctness of the Factorial Function

Proof Calculus for Total Coffectness U'U TÂP

# **Example**



BACHKHOACNCP.COM

**Program Verification** 

Nguyen An Khuong



Contents

Core Programming Language

Hoare Triples; Partial and Total Correctness

Proof Calculus for Partial Correctness

Practical Aspects of Correctness Proofs

Correctness of the Factorial Function

Proof Calculus for Total Correctness

# Nguyen An Khuong



# Contents

Core Programming Language

and Total Correctne

Proof Calculus for Partial Correctness

Practical Aspects of Correctness Proofs

Correctness of the Factorial Function

Proof Calculus for **Total Correctness** 

Homeworks

We need to be able to say that at the end, y is x!



# CHKHOACNCD

```
y = 1;
z = 0;
while (z != x) { z = z + 1; y = y * z; }
```

- We need to be able to say that at the end, y is x!
- That means we require a post-condition y = x!



BACHKHOACNCP.COM

**Program Verification** 

Nguyen An Khuong



## Contents

Core Programming Language

Hoare Triples; Partial

Proof Calculus for Partial Correctness

Practical Aspects of Correctness Proofs

Correctness of the Factorial Function

Proof Calculus for Total Correctness

# Nguyen An Khuong



# Contents

Core Programming Language

Hoare Triples; Partial

Proof Calculus for Partial Correctness

Practical Aspects of Correctness Proofs

Correctness of the Factorial Function

Proof Calculus for

Total Correctness

Homeworks

while  $(z != x) {$ Do we need pre-conditions, too?

# TÀI LIỆU SƯU TẬP

# Nguyen An Khuong



# Contents

Core Programming Language

Hoare Triples; Partial

Proof Calculus for Partial Correctness

Practical Aspects of Correctness Proofs

Correctness of the

Proof Calculus for Total Correctness

Homeworks

RACHKHOACNOP COM

y = 1; z = 0; while (z != x) { z = z + 1; y = y \* z; }
• Do we need pre-conditions, too?

Yes, they specify what needs to be the case before execution.

Example: x > 0

TÀI LIỆU SƯU TẬP



## Contents

Core Programming Language

Proof Calculus for Partial Correctness

Practical Aspects of Correctness Proofs

Correctness of the Factorial Function

Proof Calculus for Total Correctness

Homeworks

 Do we need pre-conditions, too? Yes, they specify what needs to be the case before execution.

Example: x > 0

• Do we have to prove the postcondition in one go?



# Contents

Core Programming Language

Hoare Triples; Partia

Proof Calculus for Partial Correctness

Practical Aspects of Correctness Proofs

Correctness of the Factorial Function

Proof Calculus for

Homeworks

y = 1; z = 0; while (z != x) { z = z + 1; y = y \* z; }

Do we need pre-conditions, too?
 Yes, they specify what needs to be the case before execution.

Example: x > 0

Do we have to prove the postcondition in one go?
 No, the postcondition of one line can be the pre-condition of the next!

BỞI HCMUT-CNCP

# **Assertions on Programs**

**Program Verification** 

Nguyen An Khuong



Contents

Core Programming Language

and Total Correctne

Proof Calculus for Partial Correctness

Practical Aspects of

Correctness Proofs Correctness of the

Factorial Function

Proof Calculus for **Total Correctness** 

Homeworks

Shape of assertions

# Informal meaning

If the program P is run in a state that satisfies  $\phi$ , then the state resulting from P's execution will satisfy  $\psi$ .

# (Slightly Trivial) Example

# Informal specification

Given a positive number x, the program P calculates a number y whose square is less than x.

# Assertion

$$(x > 0) P (y \cdot y < x)$$

# Example for P

$$y = 0$$

# Our first Hoare triple

BOT HCMUT-CNCP

LIÊU SƯU TÂ

$$(\!(x>0)\!) \text{ y = 0 } (\!(y\cdot y < x)\!)$$

BACHKHOACNCP.COM

**Program Verification** 

Nguyen An Khuong



# Contents

Core Programming Language

Hoare Triples; Partial and Total Correctness

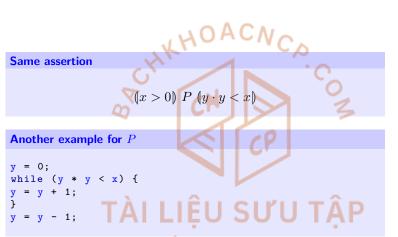
Proof Calculus for Partial Correctness

Practical Aspects of Correctness Proofs

Correctness of the Factorial Function

Proof Calculus for Total Correctness

# (Slightly Less Trivial) Example



BÓI HCMUT-CNCP

**Program Verification** 

Nguyen An Khuong



Contents

Core Programming Language

Hoare Triples: Partia and Total Correctne

Proof Calculus for Partial Correctness

Practical Aspects of Correctness Proofs

Correctness of the Factorial Function

Proof Calculus for **Total Correctness** 



# Contents

Core Programming Language

nd Total Correctne

Proof Calculus for Partial Correctness

Practical Aspects of Correctness Proofs

Correctness of the Factorial Function

Proof Calculus for Total Correctness

Homeworks

# **Definition**

Let  $\mathcal{F}$  contain function symbols and  $\mathcal{P}$  contain predicate symbols. A model  $\mathcal{M}$  for  $(\mathcal{F}, \mathcal{P})$  consists of:

- 1 A non-empty set A, the universe;
- 2 for each nullary function symbol  $f \in \mathcal{F}$  a concrete element  $f^{\mathcal{M}} \in A$ :
- 3 for each  $f \in F$  with arity n > 0, a concrete function  $f^{\mathcal{M}}:A^n\to A$ :
- 4 for each  $P \in \mathcal{P}$  with arity n > 0, a set  $P^{\mathcal{M}} \subseteq A^n$ .

# **Recall: Satisfaction Relation**

KHOACNC

The model  $\mathcal{M}$  satisfies  $\phi$  with respect to environment l, written  $\mathcal{M} \models_l \phi$ :

- in case  $\phi$  is of the form  $P(t_1,t_2,\ldots,t_n)$ , if the result  $(a_1,a_2,\ldots,a_n)$  of evaluating  $t_1,t_2,\ldots,t_n$  with respect to l is in  $P^{\mathcal{M}}$ ;
- in case  $\phi$  has the form  $\forall x \psi$ , if the  $\mathcal{M} \models_{l[x \mapsto a]} \psi$  holds for all  $a \in A$ :
- in case  $\phi$  has the form  $\exists x \psi$ , if the  $\mathcal{M} \models_{l[x \mapsto a]} \psi$  holds for some  $a \in A$ ;

**B**ỞI HCMUT-CNCP

DACHVHOACNOD COM

**Program Verification** 

Nguyen An Khuong



# Contents

Core Programming Language

Hoare Triples; Partial and Total Correctness

Proof Calculus for Partial Correctness

Practical Aspects of Correctness Proofs

Correctness of the Factorial Function

Proof Calculus for Total Correctness

Homeworks

# **Recall: Satisfaction Relation (continued)**

# KHOACNCD

- in case  $\phi$  has the form  $\neg \psi$ , if  $\mathcal{M} \models_l \psi$  does not hold;
- in case  $\phi$  has the form  $\psi_1 \vee \psi_2$ , if  $\mathcal{M} \models_l \psi_1$  holds or  $\mathcal{M} \models_l \psi_2$  holds;
- in case  $\phi$  has the form  $\psi_1 \wedge \psi_2$ , if  $\mathcal{M} \models_l \psi_1$  holds and  $\mathcal{M} \models_l \psi_2$  holds; and
- in case  $\phi$  has the form  $\psi_1 \to \psi_2$ , if  $\mathcal{M} \models_l \psi_1$  holds whenever  $\mathcal{M} \models_l \psi_2$  holds.

# TÀI LIỆU SƯU TẬP

BACHKHOACNCP.COM

**Program Verification** 

Nguyen An Khuong



Contents

Core Programming Language

Hoare Triples; Partial and Total Correctness

Proof Calculus for Partial Correctness

Practical Aspects of Correctness Proofs

Correctness of the Factorial Function

Proof Calculus for Total Correctness

# **Definition**

An assertion of the form  $(\phi) P (\psi)$  is called a Hoare triple.

- ullet  $\phi$  is called the precondition,  $\psi$  is called the postcondition.
- A state of a Core program P is a function l that assigns each variable x in P to an integer l(x).
- A state l satisfies  $\phi$  if  $\mathcal{M} \models_l \phi$ , where  $\mathcal{M}$  contains integers and gives the usual meaning to the arithmetic operations.
- Quantifiers in  $\phi$  and  $\psi$  bind only variables that do *not* occur in the program P.

BỞI HCMUT-CNCP

BACHKHOACNCP.COM

**Program Verification** 

Nguyen An Khuong



Contents

Core Programming Language

and Total Correctness

Proof Calculus for Partial Correctness

Practical Aspects of Correctness Proofs

Correctness of the Factorial Function

Proof Calculus for Total Correctness

# **Example**

**Program Verification** 

Nguyen An Khuong



# Contents

Core Programming Language

and Total Correctne

Proof Calculus for Partial Correctness

Practical Aspects of Correctness Proofs

Correctness of the

Proof Calculus for

**Total Correctness** 

Homeworks

Factorial Function

- Let l(x) = -2, l(y) = 5 and l(z) =
  - $l \models \neg(x+y < z)$
  - $l \not\models y = x \cdot z < z$
  - $l \not\models \forall u(y < u \rightarrow y \cdot z < u \cdot z)$ 
    - TÀI LIÊU SƯU TẬP



## Contents

Core Programming Language

Proof Calculus for Partial Correctness

Practical Aspects of Correctness Proofs

Correctness of the Factorial Function

Proof Calculus for Total Correctness

Homeworks

# **Definition**

We say that the triple  $(\phi) P (\psi)$  is satisfied under partial correctness if, for all states which satisfy  $\phi$ , the state resulting from P's execution satisfies  $\psi$ , provided that P terminates.

# Notation

We write  $\models_{par} (\![\phi]\!]) P (\![\psi]\!])$ .

# **Extreme Example**



BACHKHOACNCP.COM

**Program Verification** 

Nguyen An Khuong



Contents

Core Programming Language

Hoare Triples; Partial and Total Correctness

Proof Calculus for Partial Correctness

Practical Aspects of Correctness Proofs

Correctness of the Factorial Function

Proof Calculus for Total Correctness



## Contents

Core Programming Language

Hoare Triples; Partial

Proof Calculus for Partial Correctness

Practical Aspects of Correctness Proofs

Correctness of the

Proof Calculus for

Total Correctness

Homeworks

MKHOACNCD

# **Definition**

We say that the triple  $(\phi)$  P  $(\psi)$  is satisfied under total correctness if, for all states which satisfy  $\phi$ , P is guaranteed to terminate and the resulting state satisfies  $\psi$ .

# Notation

We write  $\models_{\text{tot}} (\!(\phi)\!) P(\!(\psi)\!)$ .

TÀI LIỆU SƯU TẬP

BỞI HCMUT-CNCP



BACHKHOACNCP.COM

**Program Verification** 

Nguyen An Khuong



Contents

Core Programming Language

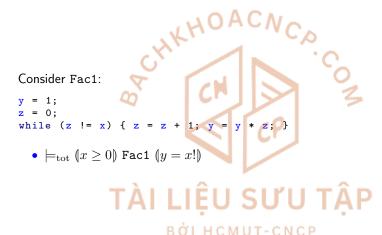
Hoare Triples; Partial

Proof Calculus for Partial Correctness

Practical Aspects of Correctness Proofs

Correctness of the Factorial Function

Proof Calculus for Total Correctness



BACHKHOACNCP.COM

**Program Verification** 

Nguyen An Khuong



## Contents

Core Programming Language

Hoare Triples; Partial and Total Correctness

Proof Calculus for Partial Correctness

Practical Aspects of Correctness Proofs

Correctness of the Factorial Function

Proof Calculus for Total Correctness





# Contents

Core Programming Language

and Total Correctne

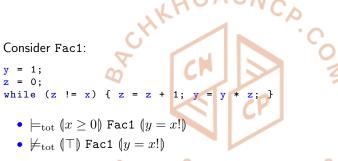
Proof Calculus for Partial Correctness

Practical Aspects of Correctness Proofs

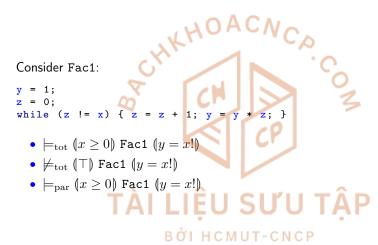
Correctness of the Factorial Function

Proof Calculus for **Total Correctness** 

Homeworks



# TÀI LIÊU SƯU TẬP BỞI HCMUT-CNCP



BACHKHOACNCP.COM

**Program Verification** 

Nguyen An Khuong



## Contents

Core Programming Language

Hoare Triples; Partial and Total Correctness

Proof Calculus for Partial Correctness

Practical Aspects of Correctness Proofs

Correctness of the Factorial Function

Proof Calculus for Total Correctness

# Program Verification Nguyen An Khuong

# BK TP.HCM

# Contents

Core Programming Language

Hoare Triples; Partial

Proof Calculus for Partial Correctness

Practical Aspects of

Correctness Proofs

Correctness of the Factorial Function

Proof Calculus for Total Correctness

Homeworks

Consider Fac1: •  $\models_{\text{tot}} (x \ge 0)$  Fac1 (y = x!)•  $\not\models_{\text{tot}} (\!(\top)\!) \text{ Fac1 } (y=x!)$ •  $\models_{\text{par}} (x \ge 0)$  Fac1 (y = x!)•  $\models_{\text{par}} (\top) \text{ Fac1 } (y = x!)$ 

BACHKHOACNCP.COM

# Nguven An Khuong



# Contents

Core Programming Language

Hoare Triples: Partial and Total Correctness

Practical Aspects of Correctness Proofs

Correctness of the Factorial Function

Proof Calculus for **Total Correctness** 

Homeworks

Core Programming Language

Hoare Triples; Partial and

3 Proof Calculus for Partial Correctness

Practical Aspects of Correctness Proofs

Correctness of the Factorial Function

Proof Calculus for Total Coffectness U'U TÂP

## Strategy

Program Verification

Nguyen An Khuong



#### Contents

Core Programming Language

Hoare Triples; Partial and Total Correctness

Proof Calculus for Partial Correctness

Practical Aspects of Correctness Proofs

Correctness of the Factorial Function

Proof Calculus for Total Correctness

Homeworks

HOACNCA

We are looking for a proof calculus that allows us to establish

$$\vdash_{\mathrm{par}} (\!(\phi)\!) P (\!(\psi)\!)$$

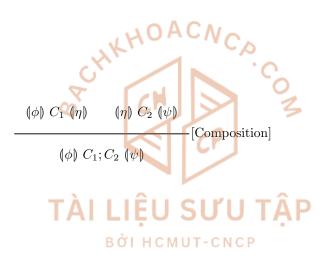
## where

- $\models_{par} (\!\!|\phi|\!\!) P (\!\!|\psi|\!\!)$  holds whenever  $\vdash_{par} (\!\!|\phi|\!\!) P (\!\!|\psi|\!\!)$  (correctness), and
- $\vdash_{par} (\!\! | \phi \!\! ) P (\!\! | \psi \!\! )$  holds whenever  $\models_{par} (\!\! | \phi \!\! ) P (\!\! | \psi \!\! )$  (completeness).

**B**ỞI HCMUT-CNCP

BACHKHOACNCP COM

## **Rules for Partial Correctness**



BACHKHOACNCP.COM

**Program Verification** 

Nguyen An Khuong



#### Contents

Core Programming Language

Hoare Triples; Partial and Total Correctness

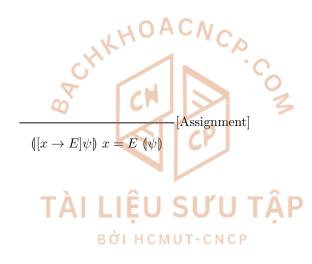
### Proof Calculus for Partial Correctness

Practical Aspects of Correctness Proofs

Correctness of the Factorial Function

Proof Calculus for Total Correctness

## **Rules for Partial Correctness (continued)**



BACHKHOACNCP.COM

**Program Verification** 

Nguyen An Khuong



#### Contents

Core Programming Language

Hoare Triples; Partial and Total Correctness

## Proof Calculus for Partial Correctness

Practical Aspects of Correctness Proofs

Correctness of the Factorial Function

Proof Calculus for Total Correctness

## **Examples**

**Program Verification** 

Nguyen An Khuong



#### Contents

Core Programming Language

Hoare Triples: Partial and Total Correctness

Practical Aspects of Correctness Proofs

Correctness of the Factorial Function

Proof Calculus for **Total Correctness** 

Homeworks

Let P be the program x = 2.

Using

 $([x \rightarrow E]\psi) \ x = E \ (\psi)$ 

we can prove:

• 
$$(2=2) P (x=2)$$

• 
$$(2=4)$$
  $P(x=4)$ 

• 
$$(2 = y) P (x = y)$$

• 
$$(2 = y) P (x = y)$$
  
•  $(2 > 0) P (x > 0)$ 

[Assignment]

BỞI HCMUT-CNCP

## More Examples

**Program Verification** 

Nguyen An Khuong



#### Contents

Core Programming Language

Hoare Triples: Partial and Total Correctness

Practical Aspects of Correctness Proofs

Correctness of the Factorial Function

Proof Calculus for **Total Correctness** 

Homeworks

Let P be the program x = x + xUsing

 $([x \to E]\psi) \ x = E(\psi)$ 

we can prove:

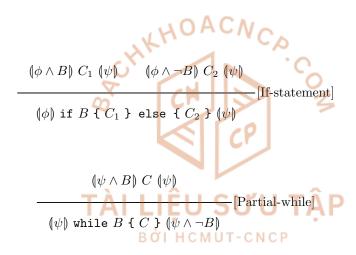
• (x+1=2) P(x=2)

• (x+1=y)P(x=y) | **EU** SU'U TÂP

BỞI HCMUT-CNCP

[Assignment]

## Rules for Partial Correctness (continued)



BACHKHOACNCP.COM

**Program Verification** 

Nguyen An Khuong



#### Contents

Core Programming Language

Hoare Triples; Partial and Total Correctness

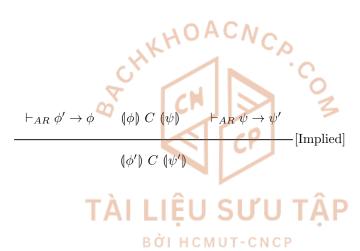
#### Proof Calculus for Partial Correctness

Practical Aspects of Correctness Proofs

Correctness of the Factorial Function

Proof Calculus for Total Correctness

## **Rules for Partial Correctness (continued)**



BACHKHOACNCP.COM

**Program Verification** 

Nguyen An Khuong



## Contents

Core Programming Language

Hoare Triples; Partial and Total Correctness

Proof Calculus for Partial Correctness

Practical Aspects of Correctness Proofs

Correctness of the Factorial Function

Proof Calculus for Total Correctness

## **Proof Tableaux**

## Proofs have tree shape

All rules have the structure

something

something else

As a result, all proofs can be written as a tree.

## **Practical concern**

These trees tend to be very wide when written out on paper. Thus we are using a linear format, called *proof tableaux*.

BACHKHOACNCP.COM

**Program Verification** 

Nguyen An Khuong



Contents

Core Programming Language

Hoare Triples; Partial and Total Correctness

Proof Calculus for Partial Correctness

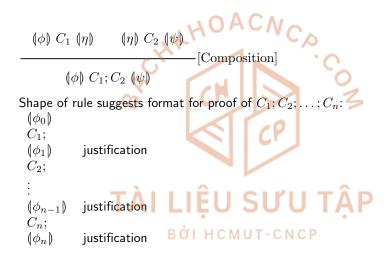
Practical Aspects of

Correctness Proofs

Correctness of the Factorial Function

Proof Calculus for Total Correctness

## Interleave Formulas with Code



BACHKHOACNCP.COM

**Program Verification** 

Nguyen An Khuong



#### Contents

Core Programming Language

Hoare Triples; Partial and Total Correctness

Proof Calculus for Partial Correctness

#### Practical Aspects of Correctness Proofs

Correctness of the Factorial Function

Proof Calculus for Total Correctness

## **Working Backwards**

## Nguven An Khuong



#### Contents

Core Programming Language

Hoare Triples: Partial and Total Correctness

Proof Calculus for Partial Correctness

#### Practical Aspects of Correctness Proofs

Correctness of the Factorial Function

Proof Calculus for Total Correctness

Homeworks

## Overall goal

Find a proof that at the end of executing a program P, some condition  $\psi$  holds.

## Common situation

If P has the shape  $C_1; \ldots; C_n$ , we need to find the weakest formula  $\psi'$  such that

 $(\psi')$   $C_n$   $(\psi)$ 

## **Terminology**

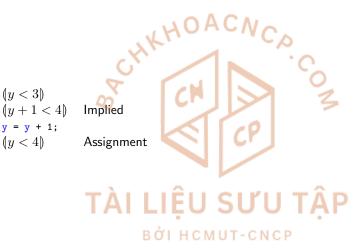
The weakest formula  $\psi'$  is called weakest precondition.

## **Example**

(y < 3)

y = y + 1;

(y < 4)



**Program Verification** 

Nguyen An Khuong



#### Contents

Core Programming Language

Hoare Triples: Partial and Total Correctness

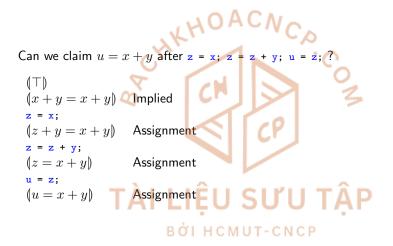
Proof Calculus for Partial Correctness

#### Practical Aspects of Correctness Proofs

Correctness of the Factorial Function

Proof Calculus for **Total Correctness** 

## **Another Example**



BACHKHOACNCP.COM

**Program Verification** 

Nguyen An Khuong



Contents

Core Programming Language

Hoare Triples; Partial and Total Correctness

Proof Calculus for Partial Correctness

Practical Aspects of Correctness Proofs

Correctness of the Factorial Function

Proof Calculus for Total Correctness

## An Alternative Rule for If

**Program Verification** 

Nguyen An Khuong



We have:

$$(\phi \wedge B) C_1 (\psi)$$
  $(\phi \wedge \neg B) C_2 (\psi)$ 
[If-statement]

$$(\!(\phi)\!)$$
 if  $B$   $\{$   $C_1$   $\}$  else  $\{$   $C_2$   $\}$   $(\!(\psi)\!)$ 

Sometimes, the following *derived rule* is more suitable:

$$(\phi_1)$$
  $C_1$   $(\psi)$   $(\phi_2)$   $C_2$   $(\psi)$ 

 $(\!(B\to\phi_1)\wedge(\neg B\to\phi_2)\!) \text{ if } B \in C_1 \text{ } \text{lelse} \in C_2 \text{ } \text{ } (\!(\psi)\!)$ 

Contents

Core Programming Language

Hoare Triples; Partial and Total Correctness

Proof Calculus for Partial Correctness

Practical Aspects of Correctness Proofs

Correctness of the Factorial Function

 $[If\text{-}stmt^{\frac{\text{Proof Calculus for}}{2}}_{\text{Homeworks}}]^{\text{Proof Calculus for}}$ 

BACHKHOACNCP.COM

## Nguyen An Khuong



#### Contents

Core Programming Language

Hoare Triples: Partial and Total Correctness

Proof Calculus for Partial Correctness

## Practical Aspects of Correctness Proofs

Correctness of the Factorial Function

Proof Calculus for **Total Correctness** 

Homeworks

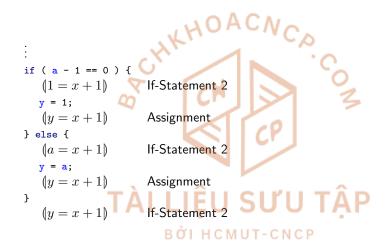
Consider this implementation of Succ:

a = x + 1;if (a - 1 == 0)else {

Can we prove ( $\top$ ) Succ (y = x + 1)? TAI LIEU SUU TÂP

BỞI HCMUT-CNCP

## **Another Example**



BACHKHOACNCP.COM

**Program Verification** 

Nguyen An Khuong



#### Contents

Core Programming Language

Hoare Triples; Partial and Total Correctness

Proof Calculus for Partial Correctness

#### Practical Aspects of Correctness Proofs

Correctness of the Factorial Function

Proof Calculus for Total Correctness

## **Another Example**

 $(x+1-1=0 \to 1=x+$  $(\neg(x+1-1=0) \to x+1=x+1)$ **Implied** a = x + 1;  $((a-1=0 \to 1=x+1) \land$  $(\neg (a-1=0) \to a=x+1)$ Assignment if (a - 1 == 0) { If-Statement 2 (1 = x + 1)v = 1: (y = x + 1)Assignment } else { (a = x + 1)v = a: B O I H C M U Assignment (y = x + 1)

**Program Verification** 

Nguyen An Khuong



Contents

Core Programming Language

Hoare Triples; Partial and Total Correctness

Proof Calculus for Partial Correctness

Practical Aspects of Correctness Proofs

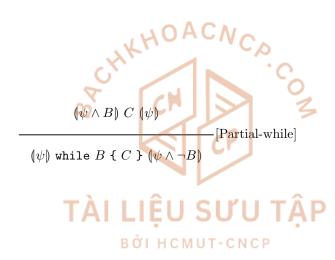
Correctness of the Factorial Function

Proof Calculus for Total Correctness

Homeworks

BACHKHOACNCP.COM

## Recall: Partial-while Rule



BACHKHOACNCP.COM

**Program Verification** 

Nguyen An Khuong



#### Contents

Core Programming Language

Hoare Triples; Partial and Total Correctness

Proof Calculus for Partial Correctness

#### Practical Aspects of Correctness Proofs

Correctness of the Factorial Function

Proof Calculus for Total Correctness

## **Factorial Example**

# KHOACNC

We shall show that the following Core program Fac1 meets this specification:

Thus, to show:

$$(\top)$$
 Fac1  $(y = x!)$ 

# TÀI LIỆU SƯU TẬP

**B**ổI HCMUT-CNCP

BACHKHOACNCP.COM

**Program Verification** 

Nguyen An Khuong



#### Contents

Core Programming Language

Hoare Triples; Partial and Total Correctness

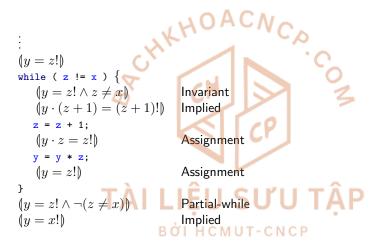
Proof Calculus for Partial Correctness

Practical Aspects of Correctness Proofs

#### Correctness of the Factorial Function

Proof Calculus for Total Correctness

## Partial Correctness of Fac1



**Program Verification** 

Nguyen An Khuong



### Contents

Core Programming Language

Hoare Triples; Partial and Total Correctness

Proof Calculus for Partial Correctness

Practical Aspects of Correctness Proofs

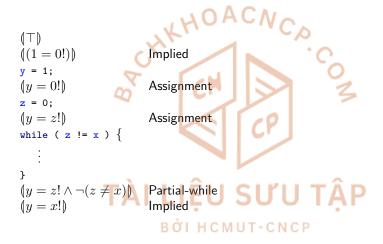
#### Correctness of the Factorial Function

Proof Calculus for Total Correctness

Homeworks

BACHKHOACNCP.COM

## Partial Correctness of Fac1



BACHKHOACNCP.COM

**Program Verification** 

Nguyen An Khuong



#### Contents

Core Programming Language

Hoare Triples; Partial and Total Correctness

Proof Calculus for Partial Correctness

Practical Aspects of Correctness Proofs

#### Correctness of the Factorial Function

Proof Calculus for Total Correctness

## Nguven An Khuong



#### Contents

Core Programming Language

Hoare Triples; Partial and Total Correctness

Proof Calculus for Partial Correctness

Practical Aspects of Correctness Proofs

Correctness of the

Factorial Function

Homeworks

Core Programming Language

Hoare Triples; Partial and

Proof Calculus for Partial Correctness

Practical Aspects of Correctness Proofs

Correctness of the Factorial Function

6 Proof Calculus for Total Correctness

BỞI HCMUT-CNCP

## Ideas for Total Correctness

**Program Verification** Nguyen An Khuong



#### Contents

Core Programming Language

Hoare Triples: Partial and Total Correctness

Proof Calculus for Partial Correctness

Practical Aspects of Correctness Proofs

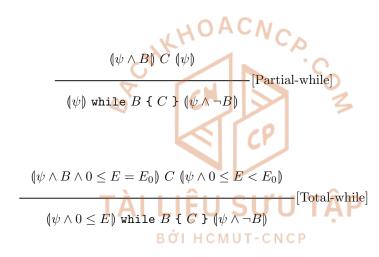
Correctness of the Factorial Function

Homeworks

- The only source of non-termination is the while command.
- If we can show that the value of an integer expression decreases in each iteration, but never becomes negative, we have proven termination. Why? Well-foundedness of natural numbers
- We shall include this argument in a new version of the while rule.

## TÀI LIÊU SƯU TẬP BỞI HCMUT-CNCP

## Rules for Partial Correctness (continued)



BACHKHOACNCP.COM

**Program Verification** 

Nguyen An Khuong



## Contents

Core Programming Language

Hoare Triples; Partial and Total Correctness

Proof Calculus for Partial Correctness

Practical Aspects of Correctness Proofs

Correctness of the Factorial Function

Proof Calculus for

## Factorial Example (Again!)



BACHKHOACNCP.COM

**B**ổI HCMUT-CNCP

**Program Verification** 

Nguyen An Khuong



#### Contents

Core Programming Language

Hoare Triples; Partial and Total Correctness

Proof Calculus for Partial Correctness

Practical Aspects of Correctness Proofs

Correctness of the Factorial Function

Proof Calculus for Total Correctness

## Factorial Example (Again!)

```
y = 1;
z = 0;
while (z != x) { z = z + 1; y = y * z; }
What could be a good variant E?
```

E must strictly decrease in the loop, but not become negative.



BACHKHOACNCP.COM

**Program Verification** 

Nguyen An Khuong



#### Contents

Core Programming Language

Hoare Triples; Partial and Total Correctness

Proof Calculus for Partial Correctness

Practical Aspects of Correctness Proofs

Correctness of the Factorial Function

Proof Calculus for

## Factorial Example (Again!)

**Program Verification** 

Nguven An Khuong



#### Contents

Core Programming Language

Hoare Triples: Partial and Total Correctness

Proof Calculus for Partial Correctness

Practical Aspects of Correctness Proofs

Correctness of the Factorial Function

Homeworks

$$z = z + 1; y = y * z;$$

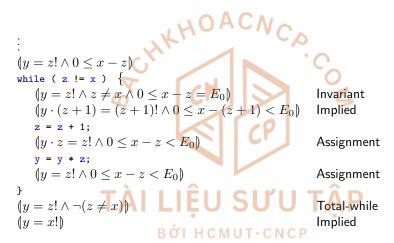
What could be a good variant E?

E must strictly decrease in the loop, but not become negative.

Answer:



## Total Correctness of Fac1



**Program Verification** 

Nguyen An Khuong



#### Contents

Core Programming Language

Hoare Triples; Partial and Total Correctness

Proof Calculus for Partial Correctness

Practical Aspects of Correctness Proofs

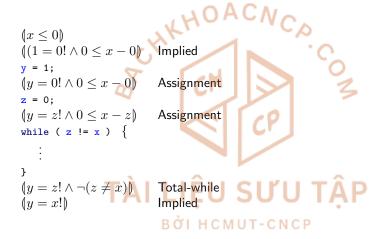
Correctness of the Factorial Function

Proof Calculus for Total Correctness

Homeworks

B A C H K H O A C N C P . C O N

## Total Correctness of Fac1



BACHKHOACNCP.COM

**Program Verification** 

Nguyen An Khuong



Contents

Core Programming Language

Hoare Triples; Partial and Total Correctness

Proof Calculus for Partial Correctness

Practical Aspects of Correctness Proofs

Correctness of the Factorial Function

Proof Calculus for Total Correctness

BACHKHOACNCP.COM

**B**ỞI HCMUT-CNCP

**Program Verification** 

Nguyen An Khuong



#### Contents

Core Programming Language

Hoare Triples; Partial and Total Correctness

Proof Calculus for Partial Correctness

Practical Aspects of Correctness Proofs

Correctness of the Factorial Function

Proof Calculus for Total Correctness